

## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1 1-48. (Cancelled)

1 49. (Currently amended) A method for managing a database system,  
2 wherein the database system includes one or more sensitive users having access to  
3 sensitive data, one or more normal users having access to non-sensitive data, one  
4 or more normal database administrators allowed to perform administrative  
5 functions over the normal user and non-sensitive data, and one or more security  
6 officers allowed to perform administrative functions over the sensitive user and  
7 sensitive data, the method comprising:

8 receiving a command to perform an administrative function ~~involving a~~  
9 ~~user on a user account~~ within the database system;

10 determining if the user account belongs to is-a sensitive user who is  
11 empowered to access sensitive data in the database system;

12 if the user account does not belong to is not-a sensitive user, and if the  
13 command is received from a normal database administrator for the database  
14 system, allowing the administrative function to proceed;

15 if the user account belongs to is-a sensitive user, and if the command is  
16 received from a normal database administrator, preventing the normal database  
17 administrator from performing the administrative function ~~involving the sensitive~~  
18 ~~user on the user account~~; and

19 if the user account belongs to is-a sensitive user, and if the command is  
20 received from a security officer within the group of one or more security officers  
21 who is the only database administrator empowered to perform administrative  
22 functions involving sensitive users, performing the administrative function on the

23 user account, wherein the one or more security officers are the only database  
24 administrators empowered to perform administrative functions on the user  
25 account.

1           50.     (Original) The method of claim 49, further comprising:  
2           receiving a request to perform an operation on a data item in the database  
3           system;  
4           if the data item is a sensitive data item containing sensitive information  
5           and if the request is received from a sensitive user who is empowered to access  
6           sensitive data, allowing the operation to proceed if the sensitive user has access  
7           rights to the sensitive data item; and  
8           if the data item is a sensitive data item and the request is received from a  
9           user who is not a sensitive user, disallowing the operation.

1           51.     (Original) The method of claim 50, wherein if the data item is a  
2           sensitive data item, if the operation is allowed to proceed, and if the operation  
3           involves retrieval of the data item, the method further comprises decrypting the  
4           data item using an encryption key after the data item is retrieved.

1           52.     (Original) The method of claim 51, wherein the encryption key is  
2           stored along with a table containing the data item.

1           53.     (Original) The method of claim 52, wherein the encryption key is  
2           stored in encrypted form.

1           54.     (Original) The method of claim 49, wherein if the user is not a  
2           sensitive user, and if the command to perform the administrative function is

3 received from a security officer, the method further comprises allowing the  
4 security officer to perform the administrative function on the user.

1 55. (Currently amended) A computer-readable storage medium storing  
2 instructions that when executed by a computer cause the computer to perform a  
3 method for managing a database system, wherein the database system includes  
4 one or more sensitive users having access to sensitive data, one or more normal  
5 users having access to non-sensitive data, one or more normal database  
6 administrators allowed to perform administrative functions over the normal user  
7 and non-sensitive data, and one or more security officers allowed to perform  
8 administrative functions over the sensitive user and sensitive data, the method  
9 comprising:

10 receiving a command to perform an administrative function ~~involving a~~  
11 ~~user on a user account~~ within the database system;

12 determining if the user ~~is~~ account belongs to a sensitive user who is  
13 empowered to access sensitive data in the database system;

14 if the user ~~is not~~ account does not belong to a sensitive user, and if the  
15 command is received from a normal database administrator for the database  
16 system, allowing the administrative function to proceed;

17 if the user account belongs to ~~is~~ a sensitive user, and if the command is  
18 received from a normal database administrator, preventing the normal database  
19 administrator from performing the administrative function ~~involving the sensitive~~  
20 ~~user on the user account~~; and

21 if the user ~~is~~ account belongs to a sensitive user, and if the command is  
22 received from a security officer within the group of one or more security  
23 officers who is the only database administrator empowered to perform  
24 administrative functions involving sensitive users, performing , performing the

25 administrative function on the user account, wherein the one or more security  
26 officers are the only database administrators empowered to perform administrative  
27 functions on the user account.

1 56. (Original) The computer-readable storage medium of claim 55,  
2 wherein the method further comprises:  
3 receiving a request to perform an operation on a data item in the database  
4 system;  
5 if the data item is a sensitive data item containing sensitive information  
6 and if the request is received from a sensitive user who is empowered to access  
7 sensitive data, allowing the operation to proceed if the sensitive user has access  
8 rights to the sensitive data item; and  
9 if the data item is a sensitive data item and the request is received from a  
10 user who is not a sensitive user, disallowing the operation.

1 57. (Original) The computer-readable storage medium of claim 56,  
2 wherein if the data item is a sensitive data item, if the operation is allowed to  
3 proceed, and if the operation involves retrieval of the data item, the method  
4 further comprises decrypting the data item using an encryption key after the data  
5 item is retrieved.

1 58. (Original) The computer-readable storage medium of claim 57,  
2 wherein the encryption key is stored along with a table containing the data item.

1 59. (Original) The computer-readable storage medium of claim 58,  
2 wherein the encryption key is stored in encrypted form.

1           60.     (Original) The computer-readable storage medium of claim 55,  
2     wherein if the user is not a sensitive user, and if the command to perform the  
3     administrative function is received from a security officer, the method further  
4     comprises allowing the security officer to perform the administrative function on  
5     the user.

1           61.     (Currently amended) An apparatus that manages a database system,  
2     wherein the database system includes one or more sensitive users having access to  
3     sensitive data, one or more normal users having access to non-sensitive data, one  
4     or more normal database administrators allowed to perform administrative  
5     functions over the normal user and non-sensitive data, and one or more security  
6     officers allowed to perform administrative functions over the sensitive user and  
7     sensitive data, comprising:

8                 a command-receiving mechanism configured to receive a command to  
9     perform an administrative function involving a user on a user account within the  
10    database system;

11                an execution mechanism configured to,  
12                         determine if the user account belongs to ~~is~~ a sensitive user  
13                         who is empowered to access sensitive data in the database system;  
14                         allow the administrative function to proceed, if the user is  
15                         ~~not~~ account does not belong to a sensitive user, and if the command  
16                         is received from a normal database administrator for the database  
17                         system;

18                        prevent a normal database administrator from performing  
19                         the administrative function ~~involving the sensitive user on the user~~  
20                         account, if the user ~~is~~ account belongs to a sensitive user, and if the

21 command is received from the normal database administrator; and  
22 to  
23 allow the administrative function to proceed, if the user is  
24 account belongs to a sensitive user, and if the command is received  
25 from a security officer within the group of one or more security  
26 officers who is the only database administrator empowered to  
27 perform administrative functions involving sensitive users, wherein  
28 the one or more security officers are the only database  
29 administrators empowered to perform administrative functions  
30 involving sensitive users.

1 62. (Previously presented) The apparatus of claim 61,  
2 wherein the command-receiving mechanism is configured to receive a  
3 request to perform an operation on a data item in the database system;  
4 wherein the execution mechanism is configured to,  
5 allow the operation to proceed, if the data item is a  
6 sensitive data item containing sensitive information and if the  
7 request is received from a sensitive user who is empowered to  
8 access sensitive data, and if the sensitive user has access rights to  
9 the sensitive data item; and to  
10 disallowing the operation, if the data item is a sensitive data  
11 item, and the request is received from a user who is not a sensitive  
12 user.

1 63. (Previously presented) The apparatus of claim 62, further  
2 comprising a decryption mechanism, wherein if the data item is a sensitive data  
3 item, if the operation is allowed to proceed, and if the operation involves retrieval

4 of the data item, the decryption mechanism is configured to decrypt the data item  
5 using an encryption key after the data item is retrieved

1 64. (Previously presented) The apparatus of claim 63, wherein the  
2 encryption key is stored along with a table containing the data item.

1 65. (Previously presented) The apparatus of claim 64, wherein the  
2 encryption key is stored in encrypted form.

1 66. (Previously presented) The apparatus of claim 61, wherein if the  
2 user is not a sensitive user, and if the command to perform the administrative  
3 function is received from a security officer, the execution mechanism is  
4 configured to allow the security officer to perform the administrative function on  
5 the user.